



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

BC2

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/240,265	01/29/1999	MARK E. PETERS	CR9-98-095	7166

25259 7590 11/29/2001

IBM CORPORATION
3039 CORNWALLIS RD.
DEPT. T81 / B503, PO BOX 12195
REASEARCH TRIANGLE PARK, NC 27709

EXAMINER

NEWTON, GREGORY A

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 11/29/2001

3

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/240,265

Applicant(s)

PETERS, MARK E.

Examiner

Gregory A Newton

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 1/29/99.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims **1-3** are rejected under 35 U.S.C. **103(a)** as being unpatentable over **Asay et al** (US 5,903,882) in view of **Reid** (US 6,131,120).

Claim 1 recites an X.509 type certificate capable of supporting more than one algorithm. For disclosure of X.509 standard authentication with multiple cryptographic algorithms, see **Reid**, e.g. column 9, line 46, and column 10, lines 28-32.

The **Reid** reference is silent with respect to explicit disclosure of alternative PKI extension for identifying at least one alternative cryptographic algorithm and providing its associated public key, and an alternative signature extension for containing a signature for the alternative cryptographic algorithm. However, teachings relating to the implementation of alternative extensions for a plurality of results are disclosed within the **Asay et al** reference of note. For disclosure of additional (alternative) extensions, see

Asay et al, column 46, last line, and top two lines of column 47. Multiple extensions are a feature of the version 3 X.509 certificates, and consequently alternative extensions for purposes such as encryption algorithms are understood to be well known in the art. The **Asay et al** reference disclosures suggest implementing the multiple combinations of encryption algorithms for X.509 certificates as taught in the **Reid** reference, with additional alternative extensions disclosed by **Asay et al** at the bottom of columns 46 and top of column 47.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings of **Asay et al** with the teachings of the **Reid** system in order to provide extensions for multiple purposes such as identification and verification by signature for the multiple cryptographic algorithms disclosed in the **Reid** system. One of ordinary skill in the art would have been motivated to do this because of availability of more memory for more algorithms to enhance security, authenticity, and validity of X.509 digital certificates as those found in Reid and Assay et al.

Furthermore, it is **well known to modify prior art by duplicating parts for multiple effects**. See St Regis Paper Co. v. Bremis Co. 193 USPQ 8 (7th Cir. 1977). (The parts in question being the duplication of extensions for algorithms in prior art X.509 certificates.)

Claim 2 recites a certificate in accordance with claim 1, with further limitations of the first cryptographic algorithm being RSA and the alternative (additional) algorithm being elliptic curve. The **Reid** reference of note suggests choosing from a variety of

encryption algorithms in column 10, line 30. The reference is silent with respect to explicit disclosure of two of the disclosed multiple encryption algorithms being RSA and elliptic curve. However, one of ordinary skill in the art would have realized that the “*such as*” delimiters in this reference at the beginning of the algorithm list (column 10, lines 30-31) would suggest elliptic curve as being a choice along with the RSA algorithm.

Claim 3 recites a certificate in accordance with claim 1, with further limitations of the certificate being able to be verified by either the signature for the first algorithm or the alternative algorithm. For disclosure of verification by signatures, see the **Asay et al** reference, e.g. column 46, second paragraph. The **Asay et al** reference is silent with respect to explicitly disclosing that the signatures correspond to separate algorithms.

However, one of ordinary skill in the art at the time of the invention would have found it obvious that the signature verification disclosed in all the references of note could be implemented in accordance with the multiple algorithm methods disclosed within the Reid reference. The multiple additional alternative extensions referred to at the bottom of column 46 and the top of column 47 of **Asay et al** would provide motivation to one of ordinary skill in the art to provide signature verification for each additional extension corresponding to multiple encryption algorithms.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Internet reference **CryptWare Toolkit**, <http://www.softwareaus.com.au/utimaco2.html>.

This reference shows a product on the market which has implemented X.509 version 3 certificates with multiple encryption algorithms. Similar to the Reid reference, this reference suggests multiple algorithms to choose from a list on the second page, e.g. RSA, DES, etc. The "etc" delimiter at the end of the list would suggest that elliptic curve could be added with RSA as a certificate with multiple encryption algorithms and associated extensions. The release dates of the CryptWare Toolkit are disclosed on the last page of that provided reference.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Gregory A Newton whose telephone number is 703-305-1373. The examiner can normally be reached on 9-6 M-F.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert DeCady can be reached on 703-305-9595. The fax phone numbers

Art Unit: 2132

for the organization where this application or proceeding is assigned are 703-746-7239 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

gn
November 17, 2001


ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100